IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Marou, J., et al.

Serial No. : 09/538,517 Group Art Unit: 2171

Filed : 3/29/00 Examiner: Bowes, S.

For : A METHOD AND SYSTEM FOR A SECURE HIGH BANDWIDTH
BUS IN A TRANSCEIVER DEVICE

BRIEF ON APPEAL

Assistant Commissioner for Patents & Trademarks
Washington, D.C. 20231

Sir:

REAL PARTY IN INTEREST

The real parties in interest are Sony Corporation and Sony Electronics Incorporated.

RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences known to appellant which will directly affect or have a bearing on the Boards decision in the present matter.

STATUS OF CLAIMS

Claims 1-44, which stand under final rejection, are currently pending and are the subject of this appeal. No other claims are pending.

STATUS OF AMENDMENTS

An Amendment was filed on March 17, 2002 in response to the Office Action mailed on November 12, 2003. The Amendment was entered. There has been no amendment after the Final Rejection mailed on May 28, 2004.

SUMMARY OF THE INVENTION

The present invention, as embodied in Claims 1 through 44, provides a method and system for implementing secure transmission of content contained in a digital broadcast signal. The system of the present invention can prevent unauthorized access to a digital data stream within the transceiver by, for example, sophisticated unauthorized users, even where such users have detailed technical knowledge of the transceiver. The system the present invention provides for secure transmission without requiring the incorporation of exotic, one-of-a-kind type components for transmitting the data between functional modules of the transceiver. The content of the digital broadcast signal is protected without requiring the imposition of multiple security schemes that impose significant cost penalties on the design and manufacture of the transceiver.

Claim 1 exemplifies one embodiment of the present invention that is implemented as a transceiver system for receiving content contained in a secure digital broadcast signal. The transceiver system uses a high bandwidth bus to transfer encrypted data between the multiple components comprising the transceiver. The data is encrypted while in transit across the bus in order to prevent access to secure content (e.g., digital broadcast signal) as the content is transferred across the bus.

Claim 1 explicitly recites a first component for generating a data stream (e.g., from a received digital broadcast signal). A first encryption unit is coupled to the first component. The first encryption unit is configured to encrypt the data stream generated from the digital broadcast signal, resulting in an encrypted data stream. Transceiver system includes a second component for generating a video signal for a display device (e.g., television, monitor, etc. to view content contained in the digital broadcast signal). A second encryption unit is coupled to the second component for decrypting the encrypted data stream received from the first component. A bidirectional digital bus is coupled to the first encryption unit and second encryption unit and functions by transferring the encrypted data stream across the bus from the first encryption unit (coupled to the first component) to the second encryption unit (coupled to the second component). A third component is coupled to the bus for arbitration of the bus to coordinate the transmission of the encrypted data stream from the first encryption unit to the second encryption unit such that content from the data stream is securely transferred from the first component to second component. This transfer across the bus takes place securely and without exposing an unencrypted data stream.

In so doing, the security of the content of the digital broadcast signal is maintained as the resulting data stream is processed by the first component and second component. The content of the digital broadcast stream is protected due to fact that the constituent data of the broadcast stream is encrypted prior to transfer across the bus. Advantageously, no copyrighted or sensitive data is exposed in the clear on the bus.

Independent Claim 13 explicitly recites a high security bus architecture for implementing secure transmission of data between components of the transceiver, as implemented in a set-top box transceiver. The architecture comprises a bus, a first encryption unit coupled to the bus for encrypting a data stream received from a first component, a second encryption unit coupled to the bus for decrypting the data stream received from the first encryption unit via the bus, and a third component coupled to the bus for arbitration of the bus to coordinate transmission of the encrypted data stream. As with the Claim 1 embodiment, the encrypted data stream is transmitted from the first encryption unit to the second encryption unit such that content from the data stream is securely transferred across the bus without exposing an unencrypted data stream.

Independent Claim 25 explicitly recites a method for implementing secure transmission of data from the digital broadcast signal between internal components of the transceiver via a bus, as implemented in a transceiver for receiving a digital broadcast signal. The method comprises accessing a digital broadcast signal using a first component of a transceiver, generating a data stream by descrambling the digital broadcast signal using the first component, and encrypting the data stream using a first encryption unit to generate an encrypted data stream. The method further comprises transmitting the encrypted data stream to a second component via a bus, and decrypting the data stream using a second encryption unit coupled to the second component such that the bus carries only an encrypted version of the data stream and advantageously without exposing an unencrypted data stream. As with the Claim 1 and Claim 13 embodiments, the encrypted

data stream is transmitted from the first encryption unit to the second encryption unit such that content from the data stream is securely transferred across the bus without exposing an unencrypted data stream.

Independent Claim 34 explicitly recites a bus architecture for a digital transceiver. In the Claim 34 embodiment, a high speed bi-directional bus is coupled to a first encryption/decryption unit (EDU). The first EDU is configured for providing decrypted digital signals to a first functional unit from the bus (e.g., incoming content for the first functional unit) and for providing encrypted digital signals to the bus from the first functional unit (e.g., outgoing content from the first functional unit). A second EDU is coupled to the bus and is configured for providing decrypted digital signals to a second functional unit from the bus (e.g., incoming content for the second functional unit) and for providing encrypted digital signals to the bus from the second functional unit (e.g., outgoing content from the second functional unit). A controller for controlling transmission of digital signals is coupled to the bus wherein audio video signals are transmitted between the first and second EDUs in encrypted form and advantageously without exposing an unencrypted data stream. Furthermore, the controller establishes encryption/decryption keys for the first and second EDUs.

ISSUES

Issue 1: Whether Claims 1-44 are patentable under 35 U.S.C. § 103 over Summers (U.S. Patent No. 6,098,133) in view of Hendricks (U.S. Patent No. 5,990,927).

Issue 2: Whether Claims 9, 23, 32, and 41 are patentable under 35 U.S.C. § 103 over Summers in view of Hendricks and in further view of Davis (U.S. Patent No. 5,805,706).

GROUPING OF CLAIMS

The rejected claims have been grouped together in each of the rejections. For each ground of rejection which Appellant contests herein and which applies to more than one claim, such additional claims, to the extent separately identified and argued below, do not stand or fall together. Appellant has shown below the reasons why these claims are separately patentable. The claims are grouped as follows:

Group 1: Claims 1-5, 7-8, 10-19, 21-30, 33-37, 39-40, and 42-44.

Group 2: Claims 6, 20, and 31.

Group 3: Claims 9, 32, 38, and 41.

ARGUMENTS

Issue 1: Whether Claims 1-44 are patentable under 35 U.S.C. § 103 over Summers (U.S. Patent No. 6,098,133) in view of Hendricks (U.S. Patent No. 5,990,927).

The following arguments are applicable to the claims in Group 1, Group 2, and Group 3.

The independent claims of the present application have been amended to explicitly recite the generation of a data stream, the encryption of the data stream, and the

secure transfer of the data stream across a bus and among components and without exposing an unencrypted data stream (emphasis added). This prevents the exposure of the unencrypted data stream for possible interception by unauthorized users.

In contrast, Summers shows an encryption system for transmitting encrypted data across a bus, but Summers does not show any special mechanisms or procedures for preventing exposure of an unencrypted data stream. Summers contemplates circuit cards in a chassis (Figure 1 of Summers). Such circuit cards are clearly not secure in the sense that they appear to take no precaution to avoid exposure of an unencrypted data stream on the computer system bus, or backplane. This renders Summers completely different from the claimed invention, and further Summers does not teach or suggest the advantages offered by the claimed invention.

In the claimed embodiments, the encryption units function by both encrypting the outgoing data streams as required and decrypting the incoming data streams as required. Hence, it should be noted that both encryption and decryption functionality is included in each unit.

Figure 3 of the present specification illustrates an example embodiment of the claimed invention. A bus 305 is coupled to the first encryption unit 311 and second encryption unit 312. The bus 305 functions by providing a high-speed, high bandwidth, bi-directional communications pathway between the AV decode block 340 and the graphics block 350. The CPU block 360 is coupled to the bus 305 in order to implement

arbitration of bus 305 to coordinate the transmission of the encrypted data stream from the first encryption unit (e.g., AV decode block 340) to the second encryption unit (Graphics Block 350). The data stream is transferred from the first encryption unit 311 of the AV decode block 340 to the second encryption unit 312 of the graphics block 350 in an encrypted form such that content from the data stream is securely transferred, without being exposed on bus 305 "in-the-clear" advantageously preventing such a vulnerable signal from interception and pirating.

Contrary to the Examiner's assertion, Summers does not show any mechanisms or procedures for preventing exposure of an unencrypted data stream as claimed. Data streams from any of the cards coupled to the bus of Summers are exposed in the clear on the bus. Summers provides no provisions that ensure no unencrypted data streams are transferred across the bus. Summers contemplates circuit cards in a chassis (Figure 1 of Summers). The circuit cards are each coupled to the PCI bus. The circuit cards transmit their information across the PCI bus in the clear. Importantly, there is no encryption of the data from a card prior to that data being transmitted across the bus. There is no decryption of the data as that data is picked up by a card from the bus.

The "secure bus arbiter" of Summers functions only as a switch that either electrically connects a card to the bus or electrically disconnects a card from the bus. The cards connect to the bus through the secure bus arbiter (e.g., multiple secure bus arbiters 203 and PCI bus 200 of Figure 1 of Summers). The secure bus arbiter "secures" data transport across the bus only by disconnecting non-permitted cards from the bus, so that

only permitted cards can communicatively access the bus (e.g., Summers Col. 3, lines 2-7, Col. 5, lines 7-13). Summers explicitly mentions cards having different classes of data as a distinguishing factor between permitted cards and non-permitted cards. For data transfers of a given class, non-permitted cards are disconnected prior to the transfer. Once the non-permitted cards are disconnected, the permitted cards transfer the data to each other across the bus.

Importantly, however, this data transfer is not encrypted. This data transfer is not encrypted by the first secure bus arbiter, sent across the bus, and decrypted by the second secure bus arbiter. There is no teaching or suggestion within Summers for such encryption, transfer the resulting encrypted data across the bus, and decryption of the encrypted data. This results in the data, whatever its class, being exposed in the clear on the bus and on the computer system backplane. This renders Summers completely different from the claimed invention and the device of Summers needs the advantages offered by the claimed invention.

The only mention of encryption in Summers is with respect to encryption prior to transmission out of the system via modem (e.g., Summers Figure 4 and Col. 5, lines 1-6). Importantly, even the data that is to be transmitted is transferred "in plain text form" across the bus.

The addition of the other cited reference, Hendricks, does not solve the deficiencies of Summers. Hendricks is relied on merely to show the generation of a video signal from a digital broadcast stream.

Because of this, the independent Claims 1, 13, 25, and 34 of the present invention are not rendered obvious by the Summers and Hendricks combination within the meaning of 35 U.S.C. Section 103.

The following arguments are applicable to the claims in Group 2.

For the rationale described above in the discussion of the claims of Group 1, Appellants assert that the combination of Summers and Hendricks does not show or suggest the generation of a data stream, the encryption of the data stream, and the secure transfer of the data stream across a bus and among components and without exposing an unencrypted data stream (emphasis added), as claimed.

In addition to the above rationale, dependent Claims 6, 20, and 31 add further separately patentable limitations describing the encryption process used to encrypt the data for transfer across the bus from the first encryption unit and decrypt the data upon reception by the second encryption unit. The encryption process is explicitly claimed as a key-based encryption process. Furthermore, the CPU is explicitly claimed as being the manager of the encryption process and distributor of the keys. This separately

patentable subject matter is not shown or suggested by the Summers and Hendricks combination.

Because of this, the Group 2 Claims 6, 20, and 31 of the present invention are not rendered obvious by the Summers and Hendricks combination within the meaning of 35 U.S.C. Section 103.

Issue 2: Whether Claims 9, 23, 32, and 41 are patentable under 35 U.S.C. § 103 over Summers in view of Hendricks and in further view of Davis (U.S. Patent No. 5,805,706).

The following arguments are applicable to the claims in Group 3.

For the rationale described above in the discussion of the claims of Group 1, Appellants assert that the combination of Summers and Hendricks does not show or suggest the generation of a data stream, the encryption of the data stream, and the secure transfer of the data stream across a bus and among components and without exposing an unencrypted data stream (emphasis added), as claimed.

In addition to the above rationale, dependent Claims 9, 23, 32, and 41 add further separately patentable limitations describing the encryption process used to encrypt the data for transfer across the bus from the first encryption unit and decrypt the data upon reception by the second encryption unit. The encryption process is explicitly claimed as

being substantially compliant with DES ECB (Data Encryption Standard Electronic Code Book).

Davis is relied upon to show encryption in accordance with DES ECB. However, Davis does not show or suggest the use of the DES ECB encryption with a first and second encryption unit in a transceiver system as in the claimed invention. For the rationale described above, the Summers-Hendricks combination does not show or suggest the generation of a data stream, the encryption of the data stream, and the secure transfer of the data stream across a bus and among components and without exposing an unencrypted data stream. The addition of Davis does not cure these defects. Thus, there is no suggestion within the references for one of ordinary skill in the art to implement any combination of the references to obtain the functionality of the claimed invention.

Because of this, the Claims 9, 23, 32, and 41 of the present invention are not rendered obvious by the Summers, Hendricks and Davis combination within the meaning of 35 U.S.C. Section 103.

To summarize, independent Claims 1, 13, 25, and 34 (e.g., the Group 1 claims) include limitations reciting the generation of a data stream, the encryption of the data stream by a first unit, and the secure transfer of the data stream across a bus and among components, the reception and decryption of the data stream by a second unit and without exposing an unencrypted data stream. Summers and Hendricks do not show or suggest these limitations. Dependent Claims 6, 20, and 31 (e.g., Group 2) add further

limitations wherein the encryption process is explicitly claimed as a key-based encryption process. Summers and Hendricks do not show or suggest these limitations. Dependent Claims 9, 23, 32, and 41 (e.g., Group 3) add further limitations wherein the encryption process is substantially compliant with DES ECB. Summers, Hendricks, and Davis do not show or suggest these limitations. Accordingly, Appellant asserts that the basis for rejecting Claims 1-44 is traversed.

CONCLUSION

Appellant believes that the pending claims 1-44 are patentable over the combination of Summers, Hendricks, and Davis. Therefore, reversal of all rejections is courteously solicited.

Dated: 11/31, 2005

Glenn Barnes
Registration No. 42,293

Two North Market Street
Third Floor
San Jose, CA 95113
(408) 938-9060

APPENDIX-Claims on Appeal

1. A transceiver system for receiving content contained in a secure digital broadcast signal, comprising:

a first component for generating a data stream;

a first encryption unit coupled to the first component, and for encrypting the data stream for transmission to generate an encrypted data stream;

a second component for generating a video signal for a display device;

a second encryption unit coupled to the second component and for decrypting the encrypted data stream received from the first component;

a bi-direcitonal digital bus coupled to the first encryption unit and the second encryption unit; and

a third component coupled to the bus for arbitration such that content from the data stream is securely transferred across the bus and without exposing an unencrypted data stream.

2. The system of Claim 1 wherein the transceiver is a set-top box.

3. The system of Claim 1 wherein the first component is an audio video decode block for decoding the data stream from a digital broadcast signal.

4. The system of Claim 1 wherein the second component is a graphics block for generating the video signal from the data stream received from the first component.

5. The system of Claim 1 wherein the third component is a CPU (central processing unit) block coupled to the bus for managing an encryption process of the first encryption unit and the second encryption unit.

6. The system of Claim 5 wherein the encryption process is key-based encryption process and the CPU block manages the distribution of keys to the first encryption unit and the second encryption unit.

7. The system of Claim 5 further comprising an arbiter coupled to the CPU block for arbitration of the bus.

8. The system of Claim 1 wherein the first component, second component, and third component include respective identification registers for identifying each component.

9. The system of Claim 1 wherein said data stream is encrypted using an encryption process substantially compliant with DES ECB (Data Encryption Standard Electronic Code Book).

10. The system of Claim 1 wherein the bus is a PCI (Peripheral Component Interconnect) compliant bus and each encryption unit performs encryption and decryption.

11. The system of Claim 1 further comprising a front end block coupled to the bus for receiving the digital broadcast signal and generating the data stream therefrom, the first component coupled to receive the data stream from the front end block via the bus.

12. The system of Claim 1 wherein the data stream is substantially compliant with a version of the MPEG (Moving Pictures Experts Group) format.

13. In a set-top box transceiver, a high security bus architecture for implementing secure transmission of data between components of the transceiver, comprising:

a bus;

a first encryption unit coupled to the bus for encrypting a data stream to generate an encrypted data stream, the data stream received from a first component;

a second encryption unit coupled to the bus for decrypting the encrypted data stream received from the first encryption unit via the bus, the data stream for transmission to a second component; and

a third component coupled to the bus for arbitration of the bus to coordinate transmission of the encrypted data stream from the first encryption unit to the second encryption unit such that content from the data stream is securely transferred across the bus and without exposing an unencrypted data stream.

14. The architecture of Claim 13 wherein the first component and the first encryption unit are built into a first integrated circuit device and the second component and the second encryption unit are built into a second integrated circuit device.

15. The architecture of Claim 13 wherein the first component is an audio video decode block for decoding the data stream from the external source.

16. The architecture of Claim 13 wherein the second component is a graphics block for generating a video signal from the data stream received from the first component.

17. The architecture of Claim 13 wherein the first component is a conditional access block for descrambling the digital broadcast signal.

18. The architecture of Claim 13 wherein the second component is an audio video decode block for decoding the data stream received from the first component.

19. The architecture of Claim 13 wherein the third component is a CPU (central processing unit) block coupled to the bus for managing an encryption process of the first encryption unit and the second encryption unit.

20. The architecture of Claim 19 wherein the encryption process is key-based encryption process and the CPU block manages the distribution of keys to the first encryption unit and the second encryption unit via the bus.

21. The architecture of Claim 19 further comprising an arbiter coupled to the CPU block for arbitration of the bus.

22. The architecture of Claim 19 wherein the first component, second component, and third component include respective identification registers for implementing component identification via the bus.

23. The architecture of Claim 19 wherein said data stream is encrypted using an encryption process substantially compliant with DES ECB (Data Encryption Standard Electronic Code Book).

24. The architecture of Claim 19 wherein the bus is a PCI (Peripheral Component Interconect) compliant bus and provides bi-directional communication between the first component and the second component.

25. In a transceiver for receiving a digital broadcast signal, a method for implementing secure transmission of data from the digital broadcast signal between internal components of the transceiver via a bus, the method comprising the steps of:

a) accessing a digital broadcast signal using a first component of a transceiver;

b) generating a data stream by descrambling the digital broadcast signal using the first component;

c) encrypting the data stream using a first encryption unit to generate an encrypted data stream;

d) transmitting the encrypted data stream to a second component via a bus; and

e) decrypting the data stream using a second encryption unit coupled to the second component such that the bus carries only an encrypted version of the data stream and without exposing an unencrypted data stream.

26. The method of Claim 25 wherein the transceiver is a set-top box.

27. The method of Claim 25 wherein the bus is a PCI (Peripheral Component Interconect) compliant bus and provides bi-directional communication between the first component and the second component.

28. The method of Claim 25 further comprising the step of decoding the data stream from the external source using an audio video decode block.

29. The method of Claim 25 further comprising the step of generating a video signal from the data stream received from the first component using a graphics block.

30. The method of Claim 25 further comprising the step of managing an encryption process of the first encryption unit and the second encryption unit using a CPU (central processing unit) block coupled to the bus.

31. The method of Claim 30 wherein the encryption process is key-based encryption process and the CPU block manages the distribution of keys to the first encryption unit and the second encryption unit.

32. The method of Claim 25 wherein said data stream is encrypted using an encryption routine substantially compliant with DES ECB (Data Encryption Standard Electronic Code Book).

33. The method of Claim 25 wherein the data stream is substantially compliant with a version of the MPEG (Moving Pictures Experts Group) format.

34. A bus architecture for a digital transceiver comprising:

a high speed bi-directional bus for communicating digital information thereon;

a first encryption/decryption unit (EDU) coupled to the bus for providing decrypted digital signals to a first functional unit from the bus and for providing encrypted digital signals to the bus from the first functional unit;

a second EDU coupled to the bus for providing decrypted digital signals to a second functional unit from the bus and for providing encrypted digital signals to the bus from the second functional unit; and

a controller for controlling transmission of digital signals on the bus wherein audio video signals are transmitted between the first and second EDUs in encrypted form, the controller also for establishing encryption/decryption keys for the first and second EDUs and without exposing an unencrypted data stream.

35. The architecture of Claim 34 wherein the first functional unit is an audio video decode block for decoding a data stream from a digital broadcast signal.

36. The architecture of Claim 34 wherein the second functional unit is a graphics block for generating a video signal from the audio video digital signals received from the first functional unit.

37. The architecture of Claim 34 wherein the controller is a CPU.

38. The architecture of Claim 34 wherein the encryption process is key-based encryption process and the controller manages the distribution of keys to the first encryption unit and the second encryption unit.

39. The architecture of Claim 34 further comprising an arbiter coupled to the controller for arbitration of the bus.

40. The architecture of Claim 34 wherein the first functional unit, second functional unit, and third functional unit include respective identification registers for identifying each functional unit.

41. The architecture of Claim 34 wherein the audio video digital signals are encrypted using an encryption process substantially compliant with DES ECB (Data Encryption Standard Electronic Code Book).

42. The architecture of Claim 34 wherein the bus is a PCI (Peripheral Component Interconnect) compliant bus.

43. The architecture of Claim 34 further comprising a front end block coupled to the bus for receiving a digital broadcast signal and generating the audio video digital signals therefrom, the first functional unit coupled to receive the audio video signals from the front end block via the bus.

44. The architecture of Claim 34 wherein the audio video digital signals are substantially compliant with a version of the MPEG (Moving Pictures Experts Group) format.